

ЗАТВЕРДЖЕНО
ЄААД.468244.185-ЛУ

Підп. та дата	
Інв. № дубл	
Взам. інв. №	
Підп. та дата	
Інв. № ориг.	

**Центр сертифікації ключів
ринку електричної енергії**

Комплексна система захисту інформації

Пояснювальна записка техноробочого проекту

ЄААД.468244.185.ПЗ

ЗМІСТ

ВСТУП.....	3
ПЕРЕЛІК СКОРОЧЕНЬ	3
1. ЗАГАЛЬНІ ПОЛОЖЕННЯ	4
1.1. Повне найменування автоматизованої системи, що розробляється.....	4
1.2. Мета створення та головне призначення КСЗІ ЦСК	4
1.3. Перелік керівних документів, на підставі яких створюється КСЗІ ЦСК.....	4
1.4. Перелік нормативно-технічних документів, що враховувались при розробці КСЗІ ЦСК.....	5
2. ОПИС ПРОЦЕСУ РОБОТИ КСЗІ ЦСК.....	5
2.1. Характеристика інформації.....	5
2.2. Категорії користувачів	6
2.3. Правила розмежування доступу	8
2.4. Функції, які виконуються КСЗІ ЦСК	9
2.5. Склад КСЗІ ЦСК	10
2.6. Заходи із захисту інформації	11
3. ОСНОВНІ ТЕХНІЧНІ РІШЕННЯ.....	12
3.1. Рішення щодо структури КСЗІ	12
3.2. Опис комплексу технічних засобів	12
3.3. Опис механізмів захисту інформації.....	15
3.4. Розміщення комплексу технічних засобів	16
3.5. Опис реалізації функціональних послуг безпеки, що реалізовані КЗЗ ЦСК.....	16

ВСТУП

У цьому документі викладені основні технічні рішення, прийняті щодо організації та складу Комплексної системи захисту інформації в центрі сертифікації ключів ринку електричної енергії, її функцій, принципів побудови та архітектури. Пропонується ряд інженерно-технічних та організаційних заходів, які повинні бути виконані на етапі створення та у процесі експлуатації КСЗІ ЦСК.

Призначений для використання особовим складом ЦСК, який бере участь у побудові КСЗІ ЦСК.

Документ може переглядатись або доповнюватися при зміні системи або вимог до неї.

ПЕРЕЛІК СКОРОЧЕНЬ

АВПЗ	Антивірусне програмне забезпечення
АРМ	Автоматизоване робоче місце
КЗЗ	Комплекс засобів захисту
КСЗІ	Комплексна система захисту інформації
ЛОМ	Локальна обчислювальна мережа
НСД	Несанкціонований доступ
ОС	Операційна система
ПБЖ	Пристрій безперебійного живлення
ПЗ	Програмне забезпечення
ПРА	Пункт реєстрації абонентів
РС	Робоча станція
СЗІ	Служба захисту інформації
СКС	Структурована кабельна система
ТЗ	Технічне завдання
ТЗІ	Технічний захист інформації
ТП	Технічний проект
ЦБД	Центральна база даних
ЦСК	Центр сертифікації ключів

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Повне найменування автоматизованої системи, що розробляється

Повне найменування: комплексна система захисту інформації центру сертифікації ключів (далі - КСЗІ ЦСК).

1.2. Мета створення та головне призначення КСЗІ ЦСК

Метою створення КСЗІ ЦСК є забезпечення захисту інформації, що обробляється, передається та зберігається в межах ЦСК від несанкціонованого доступу, порушення конфіденційності, несанкціонованої модифікації та знищення, а також забезпечення доступності зазначеної інформації для користувачів ЦСК, а саме:

- забезпечення захисту інформації, що обробляється, передається та зберігається в межах ЦСК;
- забезпечення захищеності бази даних сертифікатів ЦСК від несанкціонованого доступу та від незаконного використання персональних даних абонентів ЦСК;
- забезпечення цілісності відомостей, які знаходяться в електронному вигляді в змісті сертифікату абонента ЦСК, шляхом захисту бази даних сертифікатів ЦСК з повним обсягом відомостей про абонента, їх коректністю;
- забезпечення доступності відомостей реєстру сертифікатів у загальнодоступних каталогах (LDAP-каталогах) та на інформаційному ресурсі ЦСК (web-сайті);
- забезпечення захисту інформації при реєстрації заявників на РС адміністратора реєстрації та, РС генерації ключів користувачів, та зберіганні персональних даних заявників;
- забезпечення захисту інформації при створенні резервних копій бази даних сертифікатів ЦСК при періодичній або ініціативній актуалізації бази даних;
- забезпечення захисту інформації від порушення цілісності апаратного чи програмного забезпечення ЦСК шляхом застосування засобів технічного захисту інформації, відповідних організаційно-правових заходів.

Головним призначенням КСЗІ ЦСК є:

- захист конфіденційності, цілісності, доступності конфіденційної інформації (в тому числі персональних даних), що циркулює в ЦСК;
- захист конфіденційності, цілісності та доступності технологічної інформації щодо функціонування ЦСК, яка повинна бути доступна тільки уповноваженому персоналу, що забезпечує управління програмними та технічними засобами ЦСК;
- захист цілісності та доступності відкритої інформації, що циркулює в ЦСК.

1.3. Перелік керівних документів, на підставі яких створюється КСЗІ ЦСК

- Закон України „Про інформацію”;
- Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”;
- Закон України „Про електронний цифровий підпис”;
- Концепція технічного захисту інформації в Україні, затверджена Постановою Кабінету Міністрів України від 08.10.97 № 1126;
- Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 № 1229/99;
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;
- ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;
- ДСТУ 3918-99. Інформаційні технології. Процеси життєвого циклу програмного забезпечення;
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22;
- НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22;
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (із змінами, затвердженими наказом ДСТСЗІ СБУ № 37 від 18.06.2002).
- НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі, затверджене наказом ДСТСЗІ СБУ від 4 грудня 2000 року № 53;

- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, затверджені наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22;
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні про-філі захищеності оброблюваної інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 28 квітня 1999 року № 22;
- НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2;
- НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок ство-рення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБУ від 20 грудня 2000 року № 60;
- НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.
- Правила посиленої сертифікації, затверджені наказом ДСТСЗІ СБ України від 13.01.2005 № 3, зареєстровані в Міністерстві юстиції України від 27.01.2005 за № 104/10384 (із змінами).

1.4. Перелік нормативно-технічних документів, що враховувались при розробці КСЗІ ЦСК

- Положення про технічний захист інформації в Україні, затверджено Указом Президента України від 27 вересня 1999 року № 1229.
- Положення про державну експертизу у сфері технічного захисту інформації, затверджено наказом Держспецзв'язку від 16 травня 2007 року № 93 та зареєстровано в Міністерстві юстиції України 16 липня 2007 року за № 820/14087).
- НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
- НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
- НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
- НД ТЗІ 2.5-010-03. Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу.
- НД ТЗІ 3.7-003-2005. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.
- ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення, затверджено і введено в дію наказом Держстандарту України від 11.10.96 року № 423.
- ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт, затверджено та введено в дію наказом Держстандарту України від 19.12.96 року № 511.
- ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.
- ГОСТ 34.601-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
- ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
- ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения.

2. ОПИС ПРОЦЕСУ РОБОТИ КСЗІ ЦСК

2.1. Характеристика інформації

Відповідно до функціонального призначення у ЦСК передбачається передача, обробка та зберігання інформаційних ресурсів, які є об'єктами захисту. В таблиці 1 наведені інформаційні ресурси ЦСК, які є об'єктами захисту.

Таблиця 1

№	Позначення	Назва	Ступінь обмеження доступу
1	{Д_ТІКс}	Технологічна інформація КЗЗ ЛОМ серверів ЦСК	ІзОД
2	{Д_ТІКо}	Технологічна інформація КЗЗ РМ обслуговуючого персоналу	ІзОД
3	{Д_ТІКг}	Технологічна інформація КЗЗ РС генерації ключів	ІзОД
4	{Д_ТІУс}	Технологічна інформація управління компонентами ЛОМ серверів ЦСК	ІзОД
5	{Д_ТІУо}	Технологічна інформація управління РМ обслуговуючого персоналу	ІзОД
6	{Д_ТІУг}	Технологічна інформація управління РС генерації ключів	ІзОД
7	{Д_ЖУРС}	Журнали аудиту, що ведуться КЗЗ ЛОМ серверів ЦСК	ІзОД
8	{Д_ЖУРо}	Журнали аудиту, що ведуться КЗЗ РМ обслуговуючого персоналу	ІзОД
9	{Д_ЖУРг}	Журнали аудиту, що ведуться КЗЗ РС генерації ключів	ІзОД
10	{Д_ОКП}	Особисті ключі персоналу ІТС ЦСК	ІзОД
11	{Д_ОКЦ}	Особисті ключі ЦСК та серверів ЦСК	ІзОД
12	{Д_ОКк}	Особисті ключі заявників, що генеруються на РС генерації ключів	ІзОД (ПД)
13	{Д_КФА}	Ключова фраза автентифікації, яка може бути використана підписувачем для подання запиту на блокування/скасування свого сертифікату (по телефону)	ІзОД (ПД)
14	{Д_РП}	Реєстр підписувачів	ІзОД (ПД)
15	{Д_СЕР}	Сертифікати ЦСК, серверів ЦСК, персоналу ЦСК та користувачів ¹ , списки відкликаних сертифікатів	Відкрита
16	{Д_ВЕБ}	Загальнодоступна інформація веб-сторінки	Відкрита
17	{Д_ЗМЧ}	Запит на мітку часу	Відкрита
18	{Д_МЧ}	Мітка часу	Відкрита
19	{Д_ЗСС}	Запит статусу сертифіката	Відкрита
20	{Д_СС}	Статус сертифіката	Відкрита
21	{Д_ЗКСС}	Запит на керування статусом сертифіката	Відкрита
22	{Д_ЗКФС}	Запит на формування сертифікату	Відкрита

Технологічна інформація зберігається у вигляді постійних або тимчасових структур у пам'яті пристроїв. Технологічна інформація підлягає захисту, оскільки від неї залежить функціонування елементів ЦСК. Технологічна інформація призначена для використання адміністратором безпеки, адміністратором реєстрації, адміністратором сертифікації та системним адміністратором.

Інформація з обмеженим доступом зберігається у вигляді записів в Базі даних сертифікатів абонентів ЦСК, до якої відносяться - інформаційні об'єкти, що містять персональні дані абонентів ЦСК, інформаційні об'єкти, що містять персональні дані фахівців ЦСК та файли електронної копії бази даних ЦСК, які зберігаються у записах БД.

Відкрита інформація, до якої відносяться інформаційні об'єкти, що містять матеріали інформаційно-довідкового характеру, або ті, що не відносяться до конфіденційної інформації.

Інформація, яка надається при реєстрації заявником та яка зберігається в тілі сертифікату абонента ЦСК відноситься до інформації про особу (персональні дані). Згідно Статті 23 Закону України «Про інформацію» від 2 жовтня 1992 року №2658-ХП (враховуючи офіційне тлумачення в Рішенні Конституційного Суду України від 30.10.1997 р. № 5-зп) вказана інформація є конфіденційною.

2.2. Категорії користувачів

За рівнем повноважень відповідно до характеру та складу робіт, що виконуються в процесі функціонування ЦСК, особи, які мають доступ до технічних засобів ЦСК та інформації, що циркулює в її обчислювальній мережі, поділяються наступні категорії, які представлені в таблиці 2.

¹ Сертифікати користувачів, публікація яких на веб-сторінці або директорії ЦСК заборонений їх власниками, відносяться до ІзОД

Таблиця 2

P_AB	Адміністратор безпеки
P_AC	Системний адміністратор
P_AP	Адміністратор реєстрації
P_AЦ	Адміністратор сертифікації
P_АРЧЗ	Адміністратор реєстрації (чергова зміна)
P_ЗПП	Підписувачі
P_ЗАН	Анонімні користувачі ЦСК
P_ЗЗЯ	Заявники

Для користувачів ЦСК за виключенням P_AP, P_АРЧЗ, P_ЗПП, P_ЗАН (табл. 3) атрибутами доступу є реєстраційний запис користувача.

Таблиця 3 - Опис атрибутів доступу, що мають користувачі ІТС ЦСК згідно наданих ролей

Назва атрибуту	Роль користувача P_AB	P_AC	P_AЦ	P_AP	P_АРЧЗ	P_ЗПП	P_ЗАН	P_ЗЗЯ
Ідентифікатори локальних ролей та паролі до облікових записів ОС центральних серверів	+	+	+	+	+			
Ідентифікатори локальних ролей та паролі до облікових записів ОС серверів взаємодії	+	+	+					
Ідентифікатори локальних ролей та паролі до облікових записів ОС сервера моніторингу та синхронізації часу	+	+						
Ідентифікатори локальних ролей та паролі до облікових записів ОС РМ обслуговуючого персоналу	+	+	+	+	+			
Ідентифікатори локальних ролей та паролі до облікових записів ОС РМ віддалених адміністраторів реєстрації								
Ідентифікатори локальних адміністративних ролей та паролі до облікових записів ОС РС генерації ключів	+	+						
Ідентифікатори локальної користувальницької ролі ОС РС генерації ключів ²								+
Ідентифікатори локальних ролей та паролі до облікових записів СКБД центральних серверів	+	+						
Ідентифікатори локальних ролей та паролі до облікових записів СКБД серверів взаємодії	+	+						
Ідентифікатори локальних ролей та паролі до керованого комутаційного обладнання	+	+						
Ідентифікатори локальних ролей та паролі до облікових записів ПЗ LDAP-серверу	+	+						
Ідентифікатори локальних ролей ПК центральних серверів	+		+	+	+			
Паролі до облікових записів ПК центральних серверів	+		+					
Ідентифікатори локальних ролей та паролі до облікових записів ПК серверів взаємодії	+		+					
Назва атрибуту	Роль користувача P_AB	P_AC	P_AЦ	P_AP	P_АРЧЗ	P_ЗПП	P_ЗАН	P_ЗЗЯ

² Пароль до облікового запису ОС РС генерації ключів від імені якого запускається ПК РС генерації ключів вводиться співробітником ІТС ЦСК

Ідентифікатори локальних ролей та паролі до облікових записів ПЗ моніторингу	+	+						
Ідентифікатори локальних ролей та паролі до ЗАЗ для центральних серверів та ЗАЗ для РС генерації ключів	+							
Мережна адреса	+	+	+	+	+		+	
Особистий ключ ЕЦП			+	+	+	+		+
Пароль до особистого ключа ЕЦП			+	+	+	+		+
Сертифікат відкритого ключа			+	+	+	+		+
Ідентифікатори локальних ролей та паролі до облікових записів МЕ	+							
Ідентифікатори локальних ролей та паролі до криптомодулів	+	+	+					
Ідентифікатори локальних ролей та паролі до мережних криптомодулів								

Для інформаційних ресурсів ПТК ЦСК атрибутами доступу є:

- списки персональних ідентифікаторів користувачів, що можуть отримати доступ до кожного інформаційного ресурсу;
- тип доступу (читання, модифікація, створення, видалення об'єкта) для кожного із компонентів списку.

Адміністратор безпеки Р_АБ: здійснює адміністрування засобів захисту (крім мережних засобів захисту) та загальний контроль за станом безпеки в ЦСК, контролює відповідність налаштувань програмних та технічних засобів прийнятій політиці безпеки. Для забезпечення можливості контролю Р_АБ може мати обмежені облікові записи на всіх компонентах системи, що дозволяють йому тільки перегляд певної конфігураційної і звітної інформації на серверах та активному мережному обладнанні системи. Р_АБ має адміністративні права в операційних системах зазначених технічних засобів.

Системний адміністратор Р_АС: здійснює адміністрування веб-сервера, мережного обладнання та мережних засобів захисту, засобів, що використовуються для управління зазначеним обладнанням (сервер системи управління мережним обладнанням захисту, засоби управління, що встановлені на АРМ адміністрування активного мережного обладнання). Системний адміністратор має адміністративні права в операційних системах зазначених технічних засобів та, відповідно, повний доступ до технологічної інформації, що на них зберігається та обробляється.

Адміністратор реєстрації Р_АР: є користувач ЦСК, якій здійснює процес реєстрації заявників.

Адміністратор реєстрації (чергова зміна) Р_АРЧЗ: є користувач ЦСК, якій здійснює процес зміни статусу сертифікатів заявників.

Анонімні користувачі ЦСК - користувач ЦСК, якій має можливість перевірити статус сертифікату в Реєстрі сертифікатів та отримати Списки відкликаних сертифікатів у загальнодоступних каталогах (LDAP-каталоги). Права доступу цих користувачів повинні дозволяти створювати запити на пошук сертифікатів в загальнодоступних каталогах сертифікатів абонентів ЦСК. Читання та зберігання у окремому файлі на особистому ресурсі сертифікатів абонентів ЦСК з загальнодоступних каталогів ЦСК, що розташована на веб-сайті ЦСК.

Підписувач - кінцевий користувач ЦСК, якій є відповідальним за накладання ЕЦП на електронні документи. Права доступу цих користувачів повинні дозволяти створювати запити на пошук сертифікатів в базі даних сертифікатів абонентів ЦСК, створювати запити до ЦСК на отримання позначки часу під документом, на якому поставлений особистий підпис. Читання та зберігання у окремому файлі на особистому ресурсі сертифікатів абонентів ЦСК з бази даних ЦСК, що розташована на веб-сайті ЦСК.

Примітка. Дозволяється суміщення одним співробітником двох або більше з вищезазначених адміністративних ролей, крім ролі адміністратора безпеки.

2.3. Правила розмежування доступу

Порядок доступу до приміщень, обладнання та інформації, що циркулює в обчислювальних мережах ЦСК, особам різних категорій визначається правилами розмежування доступу, що наведені у таблиці 4.

Взаємодія суб'єктів доступу і об'єктів захисту в ПТК ЦСК здійснюється згідно з адміністративним принципом керування доступом. Тільки адміністратор безпеки має право здійснювати реєстрацію об'єктів, що підлягають захисту, призначати користувачам повноваження та права доступу. Загальні правила розмежування доступу користувачів до ресурсів визначаються наступним чином.

Таблиця 4

№	Позначення	Право доступу			
		Читання	Створення	Модифікація	Видалення ³
1	{Д_ТІКс}	P_АБ	P_АБ	P_АБ	P_АБ
2	{Д_ТІКо}	P_АБ	P_АБ	P_АБ	P_АБ
3	{Д_ТІКв}	P_ВЗІ	P_ВЗІ	P_ВЗІ	P_ВЗІ
4	{Д_ТІКг}	P_АБ	P_АБ	P_АБ	P_АБ
5	{Д_ТІУс}	P_АБ, P_АС	P_АБ, P_АС	P_АБ, P_АС	P_АБ, P_АС
6	{Д_ТІУо}	P_АБ, P_АС	P_АБ, P_АС	P_АБ, P_АС	P_АБ, P_АС
7	{Д_ТІУв}	P_ВЗІ, P_ВСА	P_ВЗІ, P_ВСА	P_ВЗІ, P_ВСА	P_ВЗІ, P_ВСА
8	{Д_ТІУг}	P_АБ, P_АС	P_АБ, P_АС	P_АБ, P_АС	P_АБ, P_АС
9	{Д_ЖУРс}	P_АБ, P_АС	-	-	P_АБ, P_АС
10	{Д_ЖУРо}	P_АБ, P_АС	-	-	P_АБ, P_АС
11	{Д_ЖУРв}	P_ВЗІ, P_ВСА	-	-	P_ВЗІ, P_ВСА
12	{Д_ЖУРг}	P_АБ, P_АС	-	-	P_АБ, P_АС
13	{Д_ОКП} ⁴	P_АЦ, P_АР, P_АРЧЗ	P_АЦ, P_АР, P_АРЧЗ	-	P_АЦ, P_АР, P_АРЧЗ
14	{Д_ОКЦ}	P_АЦ ⁵	P_АБ, P_АЦ ⁶	-	P_АБ
15	{Д_ОКк}	P_ЗЗЯ	P_ЗЗЯ	-	-
16	{Д_КФА}	P_АР, P_АРЧЗ	P_АР	P_АР	P_АР
17	{Д_РП}	P_АЦ, P_АР, P_АРЧЗ	P_АР	P_АР	P_АР
18	{Д_СЕР}	УСІ	P_АЦ	-	P_АР, P_АЦ
19	{Д_ВЕБ}	P_ЗАН, P_АЦ	P_АЦ	P_АЦ	P_АЦ
20	{Д_ЗМЧ}	-	P_ЗАН	-	-
21	{Д_МЧ}	P_АБ, P_АС	-	-	-
22	{Д_ЗСС}	-	P_ЗАН	-	-
23	{Д_СС}	P_ЗАН	-	-	-
24	{Д_ЗКСС}	P_АБ, P_АС	P_АР, P_АРЧЗ, P_ЗЗЯ	-	-
25	{Д_ЗКФС}	P_АБ, P_АС	P_АР, P_ЗЗЯ	-	-

Доступ до БД ЦСК надається адміністраторам реєстрації та сертифікації цілодобово. Технічні засоби захисту ЦСК, засоби забезпечення функціонування БД ЦСК функціонують цілодобово. Перерви в роботі ЦСК можливі лише для виконання необхідних технологічних процесів та в разі настання форс-мажорних обставин.

Обслуговуючий персонал має доступ до приміщень, в яких розташовано обладнання ЦСК, тільки в присутності адміністратора безпеки, системного адміністратора, або адміністратора реєстрації та сертифікації. Обслуговуючий персонал доступу до обладнання ЦСК не має.

2.4. Функції, які виконуються КСЗІ ЦСК

Для забезпечення необхідного рівня захисту відкритої і технологічної інформації при її зберіганні, обробці, створенні та передачі КСЗІ ЦСК реалізує:

- контроль входу (реєстрації) користувачів в систему;
- ідентифікація і автентифікація користувачів при доступі в систему;

³ Під правом "видалення" для {Д_ЖУРс}, {Д_ЖУРо}, {Д_ЖУРв}, {Д_ЖУРг} мається на увазі їх повне очищення

⁴ Кожен користувач має права доступу тільки до власного особистого ключа

⁵ Під правом "читання" мається на увазі право на ініціювання процесу з використання особистого ключа відповідним засобом КЗІ

⁶ Процедура генерації {Д_ОКЦ} здійснюється спільними зусиллями користувачів з ролями P_АБ та P_АЦ

- реєстрація спроб безпосереднього доступу користувача до об'єктів системи і непрямого доступу (зробленого процесом, який виконується на користь користувача);
- контроль коректності доступу користувачів до об'єктів системи;
- спостереження і управління доступом користувачів до об'єктів (типу файлів, каталогів, принтерів та ін.);
- визначення прав і способу доступу залежно від типу об'єкту системи;
- створення, редагування і збереження облікової інформації про користувачів, групи користувачів і об'єкти;
- спостереження і реєстрацію як системних подій (використання системи або індивідуальних додатків), так і подій, пов'язаних з безпекою системи;
- сигналізація (сповіщення) про спроби порушення захисту;
- контроль виконання встановленої політики безпеки;
- аналіз і уточнення політики безпеки;
- контроль цілісності локального і мережного програмного забезпечення (включаючи програмне забезпечення КЗЗ);
- контроль цілісності конфігурації інформаційних мереж ЦСК;
- захист від вірусів;
- управління логічною структурою інформаційних мереж ЦСК.

2.5. Склад КСЗІ ЦСК

2.5.1. Система управління КСЗІ ЦСК

Централізоване управління КСЗІ, виконання організаційних і технічних заходів із захисту інформації, модернізація КСЗІ, її експлуатація та обслуговування, підтримка працездатності технічних засобів КСЗІ, контроль за станом захищеності інформації в ЦСК здійснюється службою захисту інформації. Докладну інформацію про КСЗІ надано у Положенні про службу захисту інформації.

2.5.2. Антивірусний захист інформації

До антивірусного захисту відноситься:

- встановлення та своєчасне оновлення на АРМах ЦСК антивірусного програмного забезпечення;
- встановлення та своєчасне оновлення антивірусного програмного забезпечення на серверах ЦСК.

Для антивірусного захисту серверів ЦСК використовується ПЗ CA ESET Endpoint Security 5. Конфігурація засобів антивірусного захисту включає систему регулярних поновлень антивірусних баз. Також системні засоби антивірусного захисту реалізують можливість перевірки ресурсу за запитом (сканування компонентів файлової системи).

Для антивірусного захисту АРМів використовується ПЗ CA ESET Endpoint Security 5.

2.3.5. Технічні засоби

Реалізація наведених у п. 2.4 функцій досягається шляхом використання об'єднаних в єдину систему вбудованих послуг безпеки операційних систем робочих станцій, серверів, активного мережного обладнання, криптографічних засобів захисту, можливостей спеціалізованого і антивірусного програмного забезпечення, а також виконання спеціальних організаційних, інженерних та технологічних заходів із захисту інформації. Компоненти ЦСК, що беруть участь в реалізації політики безпеки інформації, є складовими КСЗІ ЦСК.

Для ефективного вирішення покладених на КСЗІ ЦСК завдань, система охоплює компоненти ЦСК що включає:

- робочі станції, на яких встановлено системне та прикладне програмне забезпечення для організації роботи адміністраторів;
- сервери, на яких встановлено системне програмне забезпечення для роботи системи моніторингу та керування елементами ЦСК, а також прикладне програмне забезпечення;
- структурована кабельна система (кабельна система, пасивне мережне обладнання, що об'єднує робочі станції та сервери ЦСК);
- зовнішні канали зв'язку;

- активне мережне обладнання, що забезпечує обмін даними та розмежування доступу;
- спеціалізоване мережне обладнання, яке забезпечує захист мережних об'єктів та впровадження політики безпеки (мережні засоби захисту);
- засоби криптографічного захисту інформації;
- засоби забезпечення безперервного живлення.

2.6. Заходи із захисту інформації

2.6.1. Організаційні заходи

Організаційні заходи захисту інформації - це комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту інформації шляхом регламентації діяльності персоналу і порядку функціонування засобів забезпечення інформаційної діяльності та засобів забезпечення технічного захисту інформації. З метою забезпечення безпеки інформації в ЦСК здійснено наступні заходи:

Створено Службу захисту інформації, основними завданнями якої є:

- експлуатація та обслуговування, підтримка працездатності компонентів КСЗІ;
- централізоване управління технічними засобами КСЗІ;
- контроль за станом захищеності інформації в ЦСК;
- виконання періодичних організаційних і технічних заходів із захисту інформації.

Розроблені та документовані правила забезпечення фізичного захисту обладнання ЦСК.

Розроблені та документовані правила, що регламентують доступ користувачів усіх категорій до програмно-технічних засобів ЦСК та інформації, що зберігається та обробляється в ЦСК.

Розроблені та документовані правила, що регламентують доступ сторонніх осіб до програмно-технічного комплексу ЦСК (доступ до приміщень, в яких розташовані технічні засоби).

Визначені та документовані періодичні організаційні і технічні заходи із захисту інформації.

Докладний опис зазначених організаційних заходів захисту інформації викладено у Календарному плані робіт із захисту інформації.

2.6.2. Заходи технічного захисту

До технічних заходів захисту відносяться:

- виявлення та блокування (усунення) загроз безпеці інформації за допомогою систем виявлення втручань (мережні та системного рівня);
- використання можливостей, які надаються системним та прикладним програмним забезпеченням, що використовуються в складі ЦСК, для розмежування доступу до обладнання відповідно до прав доступу, визначених у пункті 2.3.
- перевірка працездатності засобів захисту інформації;
- використання програмних засобів захисту в засобах обчислювальної техніки;
- встановлення на АРМ та серверах антивірусного ПЗ;
- своєчасне оновлення ПЗ (у тому числі антивірусного) на АРМах та серверах;
- своєчасне резервування критичних системних даних;
- використання системи гарантованого електроживлення.

3. ОСНОВНІ ТЕХНІЧНІ РІШЕННЯ

3.1. Рішення щодо структури КСЗІ

Побудова обчислювальної мережі ЦСК визначається завданнями, що вирішуються ЦСК, і зумовлює структуру КСЗІ ЦСК. В основу побудови мережі закладений модульний принцип, який дозволяє гнучко змінювати систему в частині її нарощення та перерозподілу потужності.

3.2. Опис комплексу технічних засобів

3.2.1. Проектування системи

Перед проектуванням системи було проведено обстеження технічних засобів та систем забезпечення інформаційної діяльності структурних елементів ЦСК, виявлені можливі загрози безпеці інформації, проведений їх аналіз та створена модель загроз ЦСК. На основі всебічного і повного аналізу загроз здійснений вибір необхідного переліку функціональних послуг безпеки, засобів і заходів захисту, що повинен реалізуватися КСЗІ ЦСК.

3.2.2. Склад комплексу технічних засобів

До програмно-апаратних засобів ЦСК відносяться:

- активне мережне обладнання:
 - Міжмережевий екран Cisco ASA - 5512 - 1 шт.
- засоби захисту:
 - МКМ «Гряда-301» - 2 шт;
 - КМ «Гряда-61» - 2 шт;
- серверна компонента, до складу якої входять:
 - сервери центральні ЦСК - 2 шт;
 - сервери взаємодії ЦСК - 2 шт;
 - сервер синхронізації та моніторингу - 1 шт.
 - GPS - приймач;
 - GSM - модуль.
- робочі станції, на яких встановлено системне та прикладне програмне забезпечення для організації роботи адміністраторів ЦСК;
- АРМ генерації ключів користувачів ЦСК.

3.2.3 Структурована кабельна система

Для здійснення інформаційного обміну між складовими системи побудовано СКС. Архітектура СКС приміщень ЦСК - "зірка" з мінімальною кількістю проміжних сполучень між робочими станціями та активними мережними пристроями. Елементна база системи (кросове обладнання, інсталяційний (магістральний) кабель, інформаційні розетки, кросувальні шнури) розраховані на передачу інформаційного сигналу зі смугою частот до 125МГц і придатні для побудови локальної мережі за технологією Fast Ethernet IEEE 802.3u (з пропускною здатністю каналів 100 Мбіт/с) або Gigabit Ethernet IEEE 802.3ab (з пропускною здатністю каналів 1000 Мбіт/с). Комплекс у складі ЦСК взаємодіє із зовнішньою телекомунікаційною мережею через широкосмуговий тракт зв'язку на швидкості не менше 512 кБіт/с (Передбачена можливість резервування цього тракту). Елементи СКС розташовані в межах контрольованої зони.

3.2.4 Зовнішні канали зв'язку

Обмін інформацією між Користувачами та ЦСК здійснюється орендованими каналами передачі даних.

3.2.5 Підсистема гарантованого електроживлення

Підсистема гарантованого електроживлення складається з пристроїв безперебійного живлення, розрахованих на забезпечення активного мережного обладнання, серверів, робочих місць адміністраторів та чергової зміни ЦСК електроенергією протягом 15 хвилин при 100% навантаженні, яка також призначена для захисту обладнання від зовнішніх дестабілізуючих факторів при наявності відхилень у параметрах електроживлення у вхідних мережах електропостачання.

3.2.6 Серверна компонента

Центральні сервери та сервери взаємодії функціонують автоматизовано. сервери об'єднані у відповідні кластери.

Засоби серверу ЦСК підтримують можливість автоматичного резервного копіювання реєстру сертифікатів, реєстру користувачів, бази списків відкликаних сертифікатів та бази позначок часу.

Всі технічні засоби комплексу забезпечують можливість діагностування та отримання інформації про стан їх функціонування.

РС адміністратора безпеки, системного адміністратора, адміністратора реєстрації, центральні сервери, сервери взаємодії та сервер синхронізації та моніторингу взаємодіють через внутрішню телекомунікаційну мережу на основі кабельної мережі та комутатора і утворюють ЛОМ.

3.2.7 Склад комплексу програмних засобів

До програмних засобів ЦСК відносяться:

- системне програмне забезпечення (операційні системи Microsoft Windows Server 2012 R2 Standard, Microsoft Windows 8.1 Enterprise, Linux FreeBSD 9.2 із штатним КЗЗ;
- СУБД із штатним КЗЗ та засобами їх адміністрування Microsoft SQL Server 2012 із штатним КЗЗ;
- програмний комплекс сервера ЦСК “ІІТ ЦСК-1. Ключі ЦСК”, “ІІТ ЦСК-1. CMP-сервер”, “ІІТ ЦСК-1. TSP-сервер”, “ІІТ ЦСК-1, OCSP-сервер”; “ІІТ ЦСК-1. Службові модулі сервера ЦСК”;
- HTTP-сервер Apache з модулем формування HTML-документів PHP із штатним КЗЗ;
- СУБД MySQL із штатним КЗЗ;
- LDAP-сервер Open LDAP із штатним КЗЗ;
- модуль передачі електронних поштових повідомлень (MTA) та поштовий сервер із штатним КЗЗ Exim ;
- програмний комплекс сервера взаємодії ІІТ ЦСК-1. Сервер взаємодії;
- засоби адміністрування та аудиту СУБД сервера ЦСК Microsoft SQL Server 2012 та штатні ODBC-драйвери ОС;
- засоби управління комутатором та ME Термінальний клієнт SSH, HTTPS-клієнт, окремі штатні засоби управління пристроями;
- засоби адміністрування системного ПЗ сервера взаємодії Термінальний клієнт SSH;
- програмний комплекс адміністратора сертифікації ІІТ ЦСК-1. Адміністратор сертифікації;
- програмний комплекс адміністратора реєстрації ІІТ ЦСК-1. Адміністратор реєстрації;
- програмний комплекс користувача ЦСК ІІТ Користувач ЦСК-1;
- антивірусне ПЗ: ESET Endpoint Security 5;
- інше програмне забезпечення, необхідне для функціонування системи архівації даних та захисту інформації.

3.2.8 Антивірусний захист комп'ютерних систем

Антивірусний захист комп'ютерних систем впроваджений з метою здійснення організаційних і технічних заходів щодо забезпечення захисту технічних засобів ЦСК від зараження комп'ютерними вірусами.

Антивірусний захист комп'ютерних систем призначений для захисту серверів та робочих станцій ЦСК від комп'ютерних вірусів та перекриває можливі шляхи проникнення вірусів в ЦСК через:

- файли, що виконуються;
- електронну пошту;
- системні області жорстких дисків або дискет, в тому числі і магнітно-оптичних дисків;
- документи Microsoft Word;
- електронні таблиці Microsoft Excel;
- бази даних Microsoft Access;
- презентації Microsoft PowerPoint;
- HTML сторінки із Java або Active-X аплетами;
- інші шляхи зараження .

Ефективний захист від комп'ютерних вірусів забезпечується впровадженням комплексної системи антивірусного захисту. На рівні ЦСК застосовується дворівнева система антивірусного захисту, що передбачає використання багатокomпонентності засобів антивірусного захисту на робочих станціях персонала та серверах ЦСК. Антивірусне ПЗ, що застосовується в ЦСК, відповідає вимогам ТЗІ та підтверджено у встановленому порядку.

Антивірусний захист комп'ютерних систем рівня ЦСК:

Перший рівень - захист серверів ЦСК. Антивірусне програмне забезпечення, що встановлюється на центральні сервери, виявляє спроби запису заражених, підозрілих файлів на ці сервери, на які встановлюється ПЗ CA ESET Endpoint Security 5. Антивірусні програми, які використовуються на цьому рівні, надають можливість перевірки файлів в режимі реального часу та видалення з них комп'ютерних вірусів (фоновий режим), а також перевірки за запитом адміністратора безпеки. Антивірусне програмне забезпечення дає можливість блокувати спроби запису заражених, підозрілих файлів на сервери. Кожна така спроба фіксується у протоколах, звітах антивірусної програми із зазначенням імені зараженого файлу та шляху до нього.

Другий рівень - захист автоматизованих робочих місць на робочих станціях персоналу ЦСК встановлюється антивірусне ПЗ CA ESET Endpoint Security 5, відповідність якого вимогам ТЗІ підтверджено у встановленому порядку. Дане ПЗ має у своєму складі антивірусний монітор, що запускається при вмиканні комп'ютера і працює постійно у фоновому режимі без істотного уповільнення роботи системи в цілому або окремих її додатків, а також антивірусний сканер, який здійснює перевірку за запитом користувача або адміністратора безпеки. Дана перевірка має ініціюватися при завантаженні даних із будь-яких зовнішніх носіїв інформації. Система антивірусного захисту настроєна таким чином, що відразу виліковує уражені файли в разі їх знаходження. Налаштування цього антивірусного ПЗ встановлюється за замовчуванням з серверу антивірусного захисту, оновлення встановлюються автоматично.

На рівні користувачів ЦСК система антивірусного захисту є однорівневою. На робочих станціях користувачів ЦСК встановлюється антивірусне ПЗ CA ESET Endpoint Security 5. При цьому кожного разу під час завантаження даних із будь-яких зовнішніх носіїв інформації користувачем має ініціюватися перевірка цих носіїв за допомогою антивірусного сканера.

Ведеться журнал усіх подій, які генерує антивірусне ПЗ на клієнтських робочих місцях, у якому зазначається:

- час та дата виникнення події;
- рівень події (критичний, інформаційний, попередження);
- таке ведеться журнал усіх знайдених вірусів, у якому зазначається:
- час та дату виникнення події;
- рівень події (критичний, інформаційний, попередження);
- дія, що застосовувалася до зараженого файлу;
- результат дії.

Структура програмно-технічного комплексу ЦСК наведена на рисунку 1.

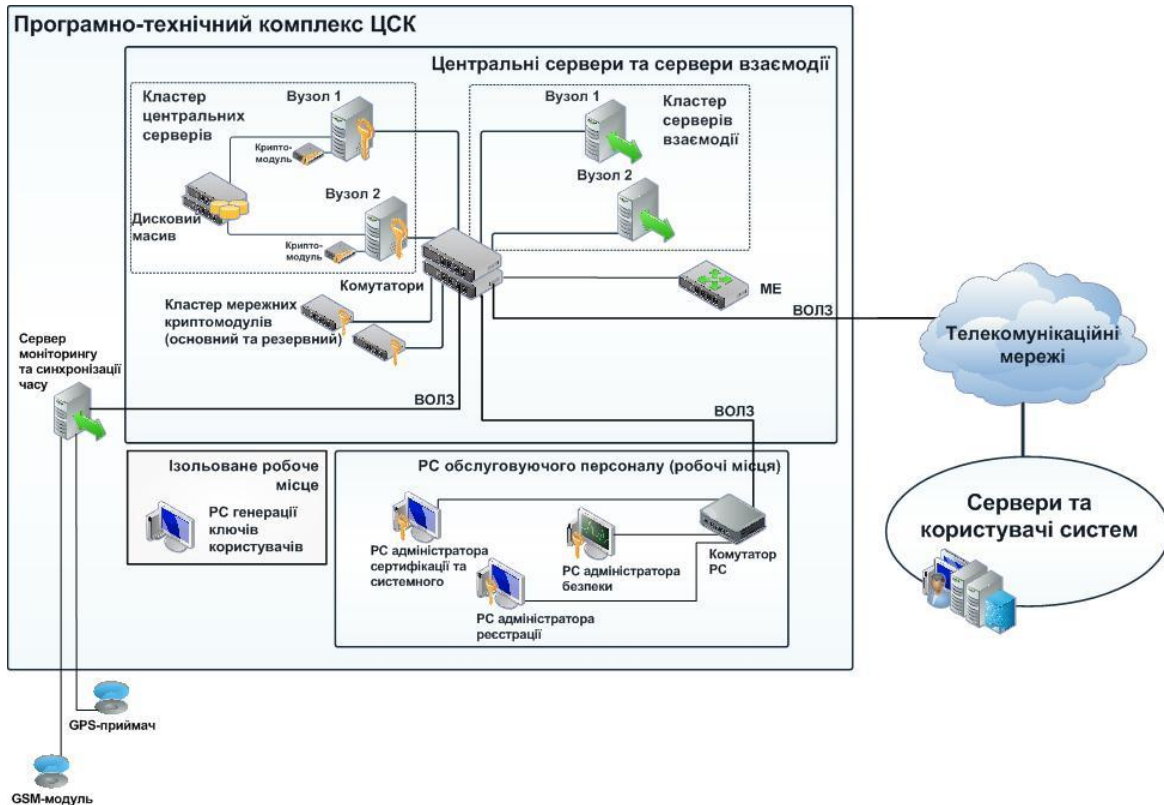


Рисунок 1. Структура програмно-технічного комплексу ЦСК

3.2.9 Концепція зберігання даних

Концепція зберігання даних включає можливість використання декількох рівнів систем зберігання для різноманітних типів даних.

Визначаються такі основних рівня зберігання даних:

- основне сховище з оперативними даними, що використовуються;
- другорядне сховище з копіями основних даних та даними, що мало використовуються.

Ці рівні системи зберігання повинні бути реалізовані в межах однієї дискової підсистеми.

Дискова система зберігання це RAID-масив із кешуванням.

Система зберігання забезпечує автоматичне зберігання даних кеш-пам'яті на дисках при відмові електричного живлення за рахунок резервних батарей.

Дискова система зберігання передбачає автоматичний, постійний контроль цілісності дисків, аналіз поганих секторів, перевірку стану резервних батарей, без втручання адміністратора та без впливу на роботу користувачів.

3.3. Опис механізмів захисту інформації

3.3.1. Серверна компонента

3.3.1.1. Механізми, що реалізовані засобами ОС

Сервери під управлінням операційної системи Microsoft Windows Server 2012 реалізують такі механізми захисту інформації за допомогою вбудованих засобів операційної системи :

- запобігання доступу неавторизованих користувачів до його внутрішніх ресурсів (шляхом налаштування параметрів конфігурації ОС);
- розмежування доступу до програм та даних сервера (реалізується засобами ОС та виконується адміністратором безпеки);
- сервери домену здійснюють автентифікацію та авторизацію користувачів ІТС на основі атрибутів доступу;
- облік інформації за допомогою ведення журналу системних подій (за допомогою служб EVENTLOG);

- фільтрація інформаційних потоків відповідно до поточної політики безпеки на основі мережних атрибутів (будь-яких полів мережних пакетів, вхідного та вихідного потоків) засобами операційної системи.

3.3.1.2. Механізми, що реалізовані засобами прикладного програмного забезпечення:

- сервери моніторингу;
- розмежування доступу до налаштувань обладнання;
- відстеження та своєчасного реагування на можливі зміни у стані роботи серверів ЦСК;
- зберігання даних моніторингу для подальшого аналізу;
- розмежування доступу до системи моніторингу на основі атрибутів доступу (ідентифікатор та пароль);
- віддалене керування обладнанням.

3.3.2. Мережні засоби захисту

Міжмережний екран Cisco ASA - 5512 реалізує такі механізми захисту інформації:

- можливість автентифікації та авторизації користувачів;
- фільтрацію інформаційних потоків відповідно до поточної політики безпеки на основі мережних атрибутів (будь-яких полів мережних пакетів, вхідного та вихідного мережного інтерфейсу);
- заборону доступу неавторизованих користувачів зовнішньої мережі до ресурсів внутрішньої мережі та навпаки;
- використання механізмів NAT для приховання справжніх мережних адрес;
- облік подій за допомогою ведення журналу системних подій (syslog) та (SNMP) на сервері моніторингу та керування обладнанням;
- розподілення на зони захисту для забезпечення розширеної політики безпеки;
- можливість застосування механізму гарячого резервування.

3.3.3. Автоматизовані робочі місця

АРМи під управлінням операційної системи Microsoft Windows 8.1 Enterprise реалізують наступні механізми захисту інформації за допомогою вбудованих засобів операційної системи:

- систему безпеки АРМ, що запобігає доступу неавторизованих користувачів до його внутрішніх ресурсів;
- антивірусний захист АРМ.

3.3.4. Програмно-апаратний засіб ідентифікації

Забезпечує можливості двофакторної автентифікації користувачів при їх доступі до ресурсів ОС АРМів та до спеціалізованого ПЗ, що передбачає взаємодію посадових осіб ЦСК з БД.

3.4. Розміщення комплексу технічних засобів

ЦСК знаходиться на технічних площах ДП "ЕНЕРГОРИНОК", що знаходяться за адресою: м. Київ, вул. Симона Петлюри, 27.

Обладнання ЦСК розміщене у пристосованих приміщеннях, укомплектованих необхідними засобами електроживлення (в тому числі пристроями безперебійного живлення), охоронною сигналізацією, пожежною сигналізацією, засобами зв'язку, допоміжними технічними засобами, системами життєзабезпечення (системи кондиціювання та опалення). Всі елементи ЦСК, за винятком каналів зв'язку, розташовані в межах контрольованої території.

З метою запобігання НСД до інформації активне мережне обладнання розміщене в монтажних шафах із замком. Доступ до приміщень ЦСК, у яких знаходяться елементи ЦСК контролюється.

3.5. Опис реалізації функціональних послуг безпеки, що реалізовані КЗЗ ЦСК

Нейтралізація загроз несанкціонованого доступу до інформації забезпечується реалізацією політики функціональних послуг, які визначаються профілем захищеності ПТК ЦСК від НСД.

Технічним завданням на КСЗІ ПТК ЦСК визначені три функціональних профілі безпеки інформації:

- функціональний профіль безпеки інформації ЛОМ ПТК ЦСК;
- функціональний профіль безпеки інформації робочої станції генерації ключів ЦСК;

- програмно-технічний комплекс взаємодії з зовнішньою телекомунікаційною мережею з рівнем гарантій оцінки коректності Г2 згідно з НД ТЗІ 2.5-004-99.

Функціональні послуги безпеки локальної обчислювальної мережі ПТК ЦСК

{КА-2, КО-1, КВ-1, ЦА-1, ЦВ-1, ДС-1, ДЗ-1, ДЗ-2, ДВ-2, ДР-1, НР-3, НИ-2, НИ-3, НК-1, НО-3, НЦ-1, НЦ-2, НТ-3, НВ-1, НА-2}.

КЗЗ РМ віддаленого адміністратора реєстрації реалізовує такий профіль захищеності:

{КА-2, КО-1, КВ-1, ЦА-1, ЦВ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1, НА-2}.

3.5.1 Специфікації вимог для КЗЗ центрального сегменту ІТС ЦСК

3.5.1.1 Базова адміністративна конфіденційність (КА-2)

КЗЗ центрального сегмента ІТС ЦСК надає адміністраторам можливість керувати потоками інформації від пасивних об'єктів захисту до об'єктів-користувачів з метою захисту пасивних об'єктів захисту від несанкціонованого ознайомлення з їх вмістом (компрометації).

Політика послуги відноситься до наступних підмножин пасивних об'єктів захисту:

- {Д_ТІКс}, {Д_ТІУс}, {Д_ЖУРс}, {Д_КФА}, {Д_РП}, {Д_СЕР} (під час їх обробки засобами ЛОМ серверів ЦСК);
- {Д_ТІКо}, {Д_ТІУо}, {Д_ЖУРо}, {Д_ОКП}, {Д_ОКЦ};
- {Д_ТІКг}, {Д_ТІУг}, {Д_ЖУРг}.

КЗЗ центрального сегменту ІТС ЦСК здійснює розмежування доступу на підставі атрибутів доступу об'єктів-користувачів і пасивних об'єктів захисту.

КЗЗ центрального сегменту ІТС ЦСК аналізує усі запити на доступ від імені об'єктів-користувачів, що надаються з метою одержання інформації, яка міститься в пасивних об'єктах захисту. КЗЗ центрального сегменту ІТС ЦСК забороняє/надає відповідний доступ згідно загальних правил розмежування доступу (таблиці 4), а також значень, що містяться у списках керування доступом.

Запити на зміну прав доступу до пасивних об'єктів захисту обробляються КЗЗ центрального сегменту ІТС ЦСК тільки у тому випадку, якщо вони надходять від користувача з роллю Р_АБ.

КЗЗ центрального сегменту ІТС ЦСК надає можливість користувачу з роллю Р_АБ визначати конкретних користувачів та/або ролі (групи користувачів) які мають право на одержання інформації, що міститься в пасивних об'єктах захисту.

Права користувачів ІТС ЦСК, на використання об'єктів-процесів, що можуть бути використані для доступу до пасивних об'єктів захисту, визначаються наявністю атрибутів доступу, що зведені до таблиці 3.

При експорті (резервному копіюванні) об'єктів {Д_ОКЦ} зберігається атрибут доступу - пароль.

3.5.1.2 Повторне використання об'єктів (КО-1)

КЗЗ центрального сегмента ІТС ЦСК забезпечує коректність повторного використання поділюваних ресурсів, гарантуючи, що у випадку, якщо поділюваний ресурс виділяється новому об'єкту-користувачу або процесу, він не містить інформації, що залишилася від попереднього об'єкта-користувача або процесу.

У якості поділюваного ресурсу розглядаються :

- оперативна пам'ять компонентів центрального сегменту ІТС ЦСК (центрального серверів, серверів взаємодії, серверу моніторингу та синхронізації часу, РМ обслуговуючого персоналу);
- тимчасові змінні ПК РМ генерації ключів в яких містяться значення {Д_ОКк}.

Перш ніж процес, що працює з правами об'єкта-користувача, зможе одержати в своє розпорядження звільнений іншим процесом пасивний об'єкт, встановлені для попереднього об'єкта-користувача або процесу права доступу до даного пасивного об'єкта скасовуються.

Перш ніж процес, що працює з правами об'єкта-користувача, зможе одержати в своє розпорядження звільнений іншим процесом пасивний об'єкт, вся інформація, що міститься в даному пасивному об'єкті, знищується.

3.5.1.3 Мінімальна конфіденційність при обміні (КВ-1)

Політика конфіденційності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, відноситься до наступних підмножин пасивних об'єктів захисту:

- {Д_ТІКс}, {Д_ТІУс}, {Д_ЖУРс}, {Д_РП}, {Д_КФА}, {Д_СЕР} (під час їх передачі між компонентами ЛОМ серверів ЦСК та РМ обслуговуючого персоналу);
- {Д_ТІКс}, {Д_ТІУс}, {Д_ЖУРс} засобів КЗІ (мережних криптомодулів, криптомодулів, АПЗ КЗІ) (під час їх передачі між відповідними засобами КЗІ та програмними засобами, що встановлені на компонентах центрального сегменту ІТС ЦСК (центральної серверах, серверах взаємодії, РМ обслуговуючого персоналу);
- {Д_РП}, {Д_КФА} (під час їх передачі між компонентами ЛОМ серверів ЦСК).

При реалізації політики послуги КЗЗ центрального сегменту ІТС ЦСК використовує:

- {Д_ОКП}, {Д_ОКЦ}, {Д_СЕР}.

Політика конфіденційності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, реалізується за рахунок використання функцій шифрування за алгоритмом ДСТУ ГОСТ 28147:2009 (режим простої заміни, режим гамування). Користувачі не мають можливості впливати на рівень захисту.

КЗЗ центрального сегменту ІТС ЦСК забезпечує захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

3.5.1.4 Мінімальна адміністративна цілісність (ЦА-1)

КЗЗ центрального сегмента ІТС ЦСК надає адміністраторам можливість керувати потоками інформації від об'єктів-користувачів до пасивних об'єктів захисту з метою захисту пасивних об'єктів захисту від несанкціонованого створення, модифікації або видалення.

Політика послуги відноситься до наступних підмножин пасивних об'єктів захисту:

- {Д_ТІКс}, {Д_ТІУс}, {Д_ЖУРс}, {Д_КФА}, {Д_РП}, {Д_СЕР}, {Д_МЧ}, {Д_ЗКСС}, {Д_ЗКФС} (під час їх обробки засобами ЛОМ серверів ЦСК);
- {Д_ТІКо}, {Д_ТІУо}, {Д_ЖУРо}, {Д_ОКП}, {Д_ОКЦ};
- {Д_ТІКг}, {Д_ТІУг}, {Д_ЖУРг}.

КЗЗ центрального сегменту ІТС ЦСК здійснює розмежування доступу на підставі атрибутів доступу об'єктів-користувачів і пасивних об'єктів захисту.

КЗЗ центрального сегменту ІТС ЦСК аналізує усі запити на доступ від імені об'єктів-користувачів, що надаються з метою модифікації інформації, яка міститься в пасивних об'єктах захисту. КЗЗ центрального сегменту ІТС ЦСК забороняє/надає відповідний доступ згідно загальних правил розмежування доступу (таблиці 4), а також значень, що містяться у списках керування доступом.

Запити на зміну прав доступу до пасивних об'єктів захисту обробляються КЗЗ центрального сегменту ІТС ЦСК тільки у тому випадку, якщо вони надходять від користувача з роллю Р_АБ.

КЗЗ центрального сегменту ІТС ЦСК надає можливість користувачу з роллю Р_АБ визначати конкретних користувачів та/або ролі (групи користувачів) які мають право на модифікацію інформації, що міститься в пасивних об'єктах захисту.

При експорті (резервному копіюванні) об'єктів {Д_ОКЦ}, {Д_ОКк} зберігається атрибут доступу - пароль. Вимог щодо збереження атрибутів доступу до інших пасивних об'єктів захисту під час їх експорту та імпорту не висувається.

3.5.1.5 Мінімальна цілісність при обміні (ЦВ-1)

Політика цілісності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, відноситься до наступних підмножин пасивних об'єктів захисту:

- {Д_ТІКс}, {Д_ТІУс}, {Д_ЖУРс}, {Д_РП}, {Д_КФА}, {Д_СЕР}, {Д_ЗКСС}, {Д_ЗКФС} (під час їх передачі між компонентами ЛОМ серверів ЦСК та РМ обслуговуючого персоналу);
- {Д_ТІКс}, {Д_ТІУс}, {Д_ЖУРс} засобів КЗІ (мережних криптомодулів, криптомодулів, АПЗ КЗІ) (під час їх передачі між відповідними засобами КЗІ та програмними засобами, що встановлені на компонентах центрального сегменту ІТС ЦСК (центральної серверах, серверах взаємодії, РМ обслуговуючого персоналу);
- {Д_РП}, {Д_КФА}, {Д_ЗКСС}, {Д_ЗКФС} (під час їх передачі між компонентами ЛОМ серверів ЦСК).

При реалізації політики послуги КЗЗ центрального сегменту ІТС ЦСК використовує:

- {Д_ОКП}, {Д_ОКЦ}, {Д_СЕР}.

Політика цілісності при обміні, що реалізується КЗЗ центрального сегменту ІТС ЦСК, реалізується за рахунок використання функцій обчислення імітовставки за алгоритмом ДСТУ ГОСТ 28147:2009. Користувачі не мають можливості впливати на рівень захисту.

КЗЗ центрального сегменту ІТС ЦСК забезпечує можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається.

3.5.1.6 Стійкість при обмежених відмовах (ДС-1)

КЗЗ центрального сегменту ІТС ЦСК забезпечує, що відмова підмножини компонентів центрального сегмента ІТС ЦСК не призведе до неможливості функціонування центрального сегмента ІТС ЦСК у цілому.

Відмова одного із задубльованих компонентів центрального сегменту ІТС ЦСК:

- ОС центральних серверів;
- ОС серверів взаємодії;
- ОС РМ обслуговуючого персоналу;
- СКБД серверів взаємодії;
- ПК центральних серверів;
- ПК серверів взаємодії;
- МЕ;
- комутаторів ЛОМ;
- мережних криптомодулів
- криптографічних модулів;

не призводить до недоступності послуг, що надаються підписувачам, заявникам та анонімним користувачам ЦСК. У гіршому випадку допускається збільшення часу їх обслуговування.

Відмова РС генерації ключів призводить лише до неможливості генерації ключів користувачів у ЦСК, але не до погіршення характеристик обслуговування інших користувачів.

Відмова сервера моніторингу та синхронізації часу призводить лише до неможливості моніторингу центрального сегменту ІТС ЦСК та неможливості синхронізації часу з сервісами точного часу.

Технічні засоби КЗЗ центрального сегменту ІТС ЦСК мають засоби індикації та/або оповіщення адміністраторів про відмову будь-якого захищеного компонента. Також ПЗ моніторингу проводить періодичну перевірку доступності основних технічних та програмних засобів, а також сигналізацію адміністраторам у випадку втрати доступності.

3.5.1.7 Модернізація (ДЗ-1)

КЗЗ центрального сегменту ІТС ЦСК надає можливість проведення модернізації компонентів центрального сегменту ІТС ЦСК, при цьому модернізація не призводить до переривання виконання КЗЗ центрального сегменту ІТС ЦСК функцій захисту та необхідності проведення додаткової державної експертизи КСЗІ.

КЗЗ центрального сегменту ІТС ЦСК надає можливість заміни/модернізації:

а) засобів КЗІ на такі самі або аналогічні засоби, за умови наявності у останніх експертного висновку Адміністрації Держспецзв'язку у сфері КЗІ та дотримання вимог визначених у ТЗ та технічних умовах на засіб КЗІ, що проходить випробування в ході державної експертизи КСЗІ в центральному сегменті ІТС ЦСК.

б) засобів ТЗІ (МЕ, комутатори ЛОМ, ЗАЗ центральних серверів, ЗАЗ для РМ генерації ключів) на такі самі або аналогічні засоби, за умови реалізації останніми функцій захисту (що вимагаються у цьому ТЗ). Відповідність функцій захисту має бути підтверджена експертним висновком Адміністрації Держспецзв'язку у сфері ТЗІ.

Заміна компонентів має бути доступна користувачам з роллю Р_АБ та/або Р_АС.

Порядок модернізації та здійснення випробувань після модернізації складу компонентів центрального сегменту ІТС ЦСК має бути визначений у методиці модернізації.

3.5.1.8 Обмежена гаряча заміна (ДЗ-2)

КЗЗ центрального сегменту ІТС ЦСК забезпечує доступність послуг і ресурсів центрального сегмента ІТС ЦСК під час заміни його окремих компонентів (за рахунок дублювання компонентів, організації кластерів).

Політика послуги поширюється на такі компоненти центрального сегменту ІТС ЦСК:

- центральні сервери;
- сервери взаємодії;

- РМ обслуговуючого персоналу;
- СКБД центральних серверів;
- СКБД серверів взаємодії;
- комутатори ЛОМ;
- мережні криптомодулі;
- криптомодулі.

Заміна компонентів доступна користувачам з роллю Р_АБ та/або Р_АС.

Модернізація не призводить до необхідності проведення додаткової державної експертизи КЗЗІ в центральному сегменті ІТС ЦСК.

3.5.1.9 Автоматизоване відновлення (ДВ-2)

КЗЗ центрального сегменту ІТС ЦСК забезпечує доступність послуг і ресурсів центрального сегмента ІТС ЦСК шляхом автоматизованого відновлення після відмов окремих компонентів, а саме:

- ОС центральних серверів;
- ОС серверів взаємодії;
- ОС сервера моніторингу та синхронізації часу;
- ОС РМ обслуговуючого персоналу;
- ОС РМ генерації ключів;
- СКБД центральних серверів;
- СКБД серверів взаємодії.

У разі неможливості відновити працездатність компонента, що відмовив, КЗЗ центрального сегменту ІТС ЦСК переводить відповідні компоненти до стану із якого повернути до нормального функціонування може тільки користувачі з роллю Р_АБ та/або Р_АС.

КЗЗ центрального сегменту ІТС ЦСК надає можливість користувачам з роллю Р_АБ та/або Р_АС відновити працездатність компонентів, що відмовили, у ручному режимі із застосуванням резервних/еталонних копій. Реалізовані ручні процедури для:

а) відновлення безпечних параметрів:

- ОС центральних серверів;
- ОС серверів взаємодії;
- ОС сервера моніторингу та синхронізації часу;
- ОС РМ обслуговуючого персоналу;
- ОС РМ генерації ключів;
- СКБД центральних серверів;
- СКБД серверів взаємодії;
- МЕ;
- комутаторів ЛОМ.

б) відновлення особистих ключів:

- мережних криптомодулів;
- криптомодулів.

3.5.1.10 Квоти (ДР-1)

КЗЗ центрального сегменту ІТС ЦСК забезпечує доступність послуг і ресурсів центрального сегмента ІТС ЦСК шляхом керування обсягом ресурсів, що виділяються користувачам.

Обмеження на ресурси СКБД центральних серверів та СКБД серверів взаємодії:

- максимальний час виконання запитів, що надходять з віддаленого вузла;
- максимальна кількість конкурентних з'єднань.

Обмеження на ресурси ПЗ HTTP-серверу:

- максимальна кількість користувачів, що можуть одночасно отримувати доступ до ПЗ HTTP-серверу;
- кількість обробників запитів користувачів ПЗ HTTP-серверу.

Запити на зміну встановлених обмежень обробляються КЗЗ центрального сегменту ІТС ЦСК тільки в тому випадку, якщо вони надходять від Р_АБ або Р_АС.

3.5.1.11 Сигналізація про небезпеку (НР-3)

КЗЗ центрального сегменту ІТС ЦСК здійснює реєстрацію подій, що мають безпосереднє відношення до безпеки, а саме:

- отримання чи спроба отримання користувачем доступу (будь-якого виду) до об'єктів захисту;
- результати ідентифікації та автентифікації користувачів ІТС ЦСК;
- викриття порушення цілісності або відмова компонентів, що входять до складу центрального сегменту ІТС ЦСК;
- відновлення працездатності компонентів, що входять до складу центрального сегменту ІТС ЦСК.

Журнал реєстрації містить інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації містить інформацію, достатню для встановлення користувача (об'єкта-користувача), програмного засобу зі складу центрального сегменту ІТС ЦСК, що мали відношення до кожної зареєстрованої події

КЗЗ центрального сегменту ІТС ЦСК контролює одиничні або повторювані реєстраційні події, які можуть свідчити про прямі (істотні) порушення політики безпеки ІТС ЦСК, а саме відмова компонентів, що входять до складу центрального сегменту ІТС ЦСК.

КЗЗ центрального сегменту ІТС ЦСК негайно інформує користувачів з ролями Р_АБ, Р_АС про події засобами електронної пошти/мобільного зв'язку (sms).

Користувачі з ролями Р_АБ, Р_АС мають в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

КЗЗ центрального сегменту ІТС ЦСК забезпечує захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування. Заборонено редагування вмісту журналів реєстрації. Єдиною операцією, що визначена над об'єктам типу журнал реєстрації, що призводить до зміни її вмісту має бути повне очищення.

3.5.1.12 Одиночна ідентифікація і автентифікація (НИ-2)

КЗЗ центрального сегменту ІТС ЦСК визначає і перевіряє особистість користувача, що намагається одержати доступ до апаратно-програмних та апаратних компонентів ІТС ЦСК шляхом безпосереднього підключення або підключення через контрольоване середовище.

Атрибути, що використовується для ідентифікації та автентифікації користувачів у компонентах центрального сегмента ІТС ЦСК наведені у таблиці 3.

Послуга реалізується КЗЗ центрального ІТС ЦСК із застосуванням захищеного механізму одного з типів:

- "знання чогось", а саме: логін та/або пароль;
- "володіння чимось", а саме: АПЗ КЗІ.

Кожний користувач, до якого відноситься політика послуги, повинен однозначно ідентифікуватися КЗЗ центрального сегмента ІТС ЦСК.

КЗЗ центрального сегменту ІТС ЦСК забезпечує захист даних автентифікації від несанкціонованого читання та модифікації.

3.5.1.13 Множина ідентифікація і автентифікація (НИ-3)

КЗЗ центрального сегменту ІТС ЦСК визначає і перевіряє особистість користувача, що намагається одержати доступ до апаратно-програмних та апаратних компонентів ІТС ЦСК шляхом підключення через неконтрольоване середовище.

Атрибути, що використовується для ідентифікації та автентифікації користувачів у компонентах центрального сегмента ІТС ЦСК наведені у таблиці 3.

Послуга реалізується КЗЗ центрального сегмента ІТС ЦСК із одночасним застосуванням захищених механізму таких типів:

- "знання чогось", а саме: логін та/або пароль;
- "володіння чимось", а саме: АПЗ КЗІ.

Кожний користувач, до якого відноситься політика послуги, повинен однозначно ідентифікуватися КЗЗ центрального сегмента ІТС ЦСК.

КЗЗ центрального сегменту ІТС ЦСК забезпечує захист даних автентифікації від несанкціонованого читання та модифікації.

3.5.1.14 Однонаправлений достовірний канал (НК-1)

КЗЗ центрального сегменту ІТС ЦСК гарантує користувачам можливість безпосередньої взаємодії з ним.

Політика послуги поширюється на:

- внутрішніх користувачів усіх категорій;
- заявників.

Встановлення достовірного зв'язку між користувачем до якого поширюється політика послуги, і КЗЗ центрального сегменту ІТС ЦСК, здійснюється з використанням захищеного (від перехоплення чи підміни) механізму введення користувачем свого паролю.

Достовірний канал використовується для початкової ідентифікації і автентифікації користувачів, до яких відноситься політика послуги. Зв'язок з використанням даного каналу ініціюється виключно користувачем.

3.5.1.15 Розподіл обов'язків на підставі привілеїв (НО-3)

КЗЗ центрального сегменту ІТС ЦСК підтримує :

- адміністративні ролі (P_АБ, P_АС);
- користувальницькі ролі (P_АР, P_АЦ, P_ЗПП, P_ЗАН, P_ЗЗЯ).

Користувач ІТС ЦСК має можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

3.5.1.16 КЗЗ з контролем цілісності (НЦ-1)

КЗЗ центрального сегменту ІТС ЦСК реалізує механізми контролю цілісності підмножини своїх компонентів з метою виявлення фактів їх несанкціонованої модифікації.

Політика послуги поширюється на:

- ЗАЗ центральних серверів;
- МЕ;
- комутатори ЛОМ;
- мережні криптомодулі;
- криптомодулі;
- АПЗ КЗІ;
- ПЗ користувача ЦСК;
- ЗАЗ для РМ генерації ключів.

У разі виявлення порушення цілісності свого компоненту КЗЗ центрального сегменту ІТС ЦСК повідомляє користувача з роллю P_АБ або P_АС і переводить об'єкт, цілісність якого було порушено, до стану з якого повернути його до нормального функціонування може тільки користувач з роллю P_АБ або P_АС.

За допомогою організаційних заходів забезпечено неможливість завантаження серверів та робочих місць зі складу комплексу технічних засобів центрального сегменту ІТС ЦСК із зовнішніх носіїв або через мережевий інтерфейс.

3.5.1.17 КЗЗ з гарантованою цілісністю (НЦ-2)

КЗЗ центрального сегменту ІТС ЦСК підтримує домен для виконання підмножини своїх компонентів з метою захисту від зовнішніх впливів і несанкціонованої модифікації та/або втрати керування.

Політика послуги поширюється на:

- КЗЗ ОС центральних серверів;
- КЗЗ ОС серверів взаємодії;
- КЗЗ ОС сервера моніторингу та синхронізації часу;
- КЗЗ ОС РМ обслуговуючого персоналу;
- КЗЗ ОС РМ генерації ключів

та усі програмні засоби, що входять до складу КЗЗ центрального сегменту ІТС ЦСК та функціонують під їх керуванням.

За допомогою організаційних заходів забезпечено неможливість завантаження серверів та робочих місць зі складу комплексу технічних засобів центрального сегменту ІТС ЦСК із зовнішніх носіїв або через мережевий інтерфейс.

3.5.1.18 Самотестування в реальному часі (НТ-3)

КЗЗ центрального сегменту ІТС ЦСК перевіряє і на підставі цього гарантує правильність функціонування і цілісність певної множини функцій КЗЗ центрального сегменту ІТС ЦСК.

Процедурами, що використовуються для оцінки правильності функціонування КЗЗ центрального сегменту ІТС ЦСК є:

- тестування на предмет вірусного зараження;
- перевірка коректності конфігураційних файлів окремих програмних засобів;
- тестування правильності криптографічних перетворень, що реалізовані у засобах КЗІ зі складу КЗЗ центрального сегменту ІТС ЦСК;
- діагностика функціонування мережних вузлів та перевірка функціонування спеціалізованих програмних сервісів.

КЗЗ центрального сегменту ІТС ЦСК здатний виконувати набір тестів з метою оцінки правильності функціонування. Тести виконуються при запуску та за запитом користувача з роллю Р_АБ, Р_АС або іншого уповноваженого користувача.

3.5.1.19 Автентифікація вузла (НВ-1)

КЗЗ центрального сегмента ІТС ЦСК перед початком обміну забезпечує :

- ідентифікацію та автентифікацію КЗЗ РМ віддаленого адміністратора реєстрації;
- взаємну ідентифікацію та автентифікацію апаратно-програмних засобів КЗІ (мережні криптомодулі, криптомодулі, АПЗ КЗІ) та програмних засобів, що встановлені на компонентах центрального сегменту ІТС ЦСК (центральному серверу, серверах взаємодії, РМ обслуговуючого персоналу).

Атрибутами доступу, що використовуються при реалізації послуги є особистий і відкритий (у складі сертифіката) ключі електронного цифрового підпису компонентів КЗЗ ІТС ЦСК, що взаємодіють.

Підтвердження ідентичності здійснюється на основі затвердженого протоколу автентифікації, що використовує механізм ЕЦП.

3.5.1.20 Автентифікація відправника з підтвердженням (НА-2)

КЗЗ центрального сегмента ІТС ЦСК забезпечує захист від відмови від авторства і однозначно встановлює належність певного об'єкта певному користувачу (процесу), тобто той факт, що об'єкт був створений певним користувачем (процесом).

Політика послуги відноситься до:

- користувачів з ролями: Р_АЦ, Р_АР, Р_ВАР, Р_ЗПП, Р_ЗЗЯ;
- процесів: ПК центрального сервера;
- об'єктів захисту: {Д_СЕР}, {Д_МЧ}, {Д_ЗКСС}, {Д_ЗКФС}.

Атрибутом, що дозволяє однозначно встановити, що об'єкти захисту до яких відноситься політика послуги, були створені одним з користувачів (процесів) до яких відноситься політика послуги є ЕЦП.

Атрибутами користувачів (процесів) на яких поширюється політика послуги є особистий ключ ЕЦП та сертифікат відкритого ключа.

Процедурою, що дозволяє однозначно встановити, що об'єкт захисту був створений певним користувачем (процесом), є перевірка ЕЦП від даних, що перевіряються за криптографічним алгоритмом ЕЦП, що визначений ДСТУ 4145-2002. Для забезпечення можливості однозначного підтвердження належності об'єкта незалежною третьою стороною, у складі КЗЗ центрального сегмента ІТС ЦСК при формуванні та перевірці ЕЦП використовуються надійні засоби ЕЦП та посилені сертифікати відкритих ключів.

У якості незалежної третьої сторони виступає акредитований центр сертифікації ключів.

3.5.2 Заходи захисту від витоку інформації по каналах ПЕМВН та від спеціальних впливів

3.5.2.1 Центральні сервери та криптомодулі розміщені у екранованій шафі, яка відповідає вимогам Додатку 1 до Правил посиленої сертифікації.

3.5.2.2 Електроживлення центрального сервера та криптомодуля здійснюється через фільтри електроживлення, які відповідають вимогам Додатку 1 до Правил посиленої сертифікації.

3.5.2.3 Для з'єднання обладнання, яке знаходиться у екранованій шафі, з обладнанням, яке знаходиться за межами екранованої шафи, використовуються оптоволоконні лінії зв'язку.